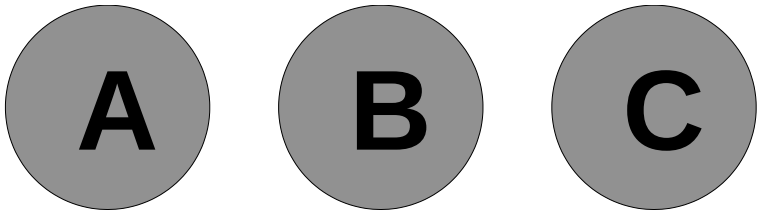

GUIDANCE MATERIAL

SSA Evaluation Activities

1 Introduction

This chapter gives practical guidance on verifying and validating a System Safety Assessment (SSA).

The guidance is meant to be used with the SAM and aims to avoid duplication. For the most part, the guidance gives references to specific parts of the SAM but there are occasional quotes to reduce the reader's time spent searching for information.

2 Objectives of the SSA

SSA is a process initiated at the beginning of the implementation of an Air Navigation System (ANS). The objective of performing a SSA is to **demonstrate** that the system, as implemented, achieves an acceptable (or at least a tolerable) risk and consequently satisfies its Safety Objectives specified in the Functional Hazard Assessment (FHA) and the system elements meet their Safety Requirements specified in the Preliminary System Safety Assessment (PSSA).

The SSA process **collects evidences** and **provides assurance** from implementation to decommissioning that the system achieves an acceptable (or at least a tolerable)

risk and consequently satisfies its Safety Objectives and that the system elements meet their Safety Requirements.

3 How to Apply the Evaluation Process

Verification and validation processes are satisfied through a combination of reviews and analysis of the SSA output. One distinction between reviews and analysis is that analysis provides repeatable evidence of correctness and reviews provide a qualitative assessment of correctness. A review may consist of an inspection of an output of a SAM process guided by a checklist or similar aid. An analysis may examine in detail the performance, results and traceability of the SAM process.

The person (or persons) carrying out verification and validation will report to the project manager. Their role will be to give the project manager an objective evaluation of the outputs of the SSA and the process followed.

The accomplishment of objective evaluation is more likely to be ensured when the verification and validation processes are carried out by a person (or persons) other than those who performed the SSA process. However, such independence should only be necessary for the most critical systems – as determined during the FHA. The involvement of people with different skills (ATCO's, Pilots & Engineers) in a SAM process (e.g. testing a system) will by itself ensure a degree of objectivity. Verification and validation may be carried out by the same person, something which the project manager will decide in accordance with the Safety Management System implemented within the organisation.

The verification and validation processes are split into five separate processes to match the life-cycle phases as there will be a significant time span between some of these phases, and different personnel will be involved. The processes are outlined in the following paragraphs covering:

- System Implementation and Integration;
- Transfer to Operations;
- Operations and Maintenance;
- System Change;
- Decommissioning.

Note that the verification and validation activities have to take place in phase with the development of the SSA

4 Scope of these Guidelines

The activities described are limited to the verification and validation of SSA outputs.

5 SSA Verification

5.1 Objective

The verification task reviews and analyses the results of the SSA ensuring that the information and output required from the SSA is available (e.g. "getting the output right"). The main focus of the task is the documented results of the Safety Assurance and Evidence Collection (SAEC) carried out during the SSA. The SAEC activity itself involves a considerable amount of verification at each stage.

5.2 System implementation and integration verification process

The purpose of verification for this phase is to provide assurance that the system, as implemented, is able to achieve an acceptable level of risk, that is to meet its Safety Objectives and that the system elements (human, procedure and equipment) meet their Safety Requirements (including assurance levels).

The verification goals are summarised in the following figure. The numbers refer to the location of guidance (in this document) on each goal in the tables which follow.

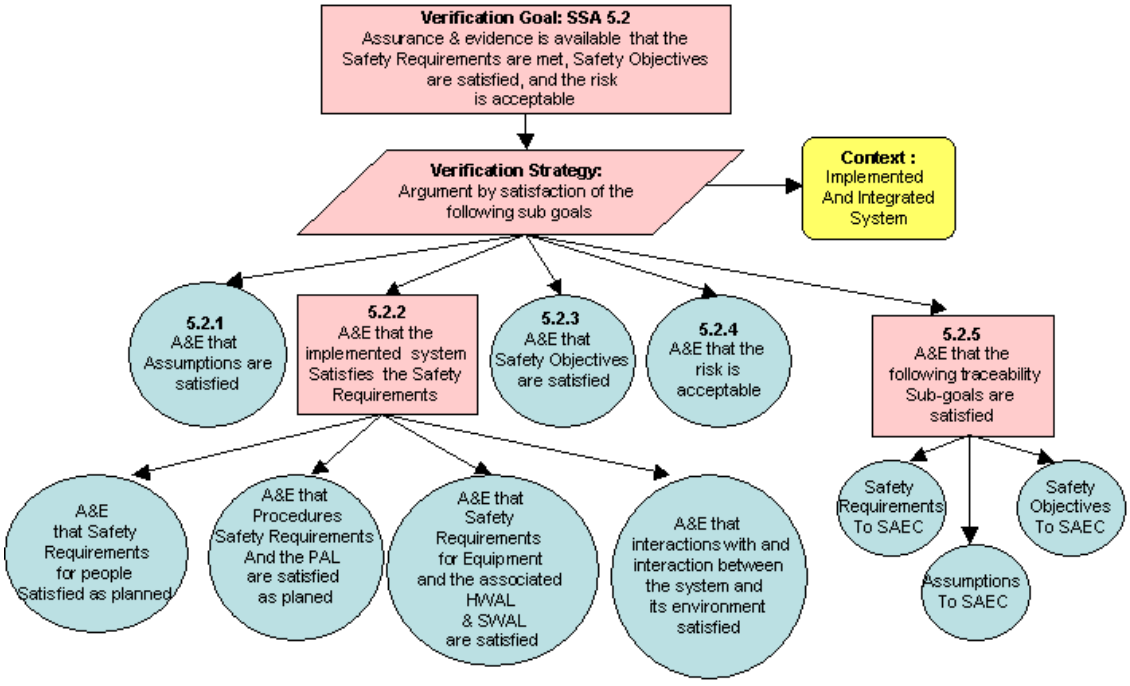

Figure 5.2 Verification goals

The reviewer will need the correct version of the following information for conducting the verification:

- A description of the high level functions of the system, with their associated Safety Objectives and a list of hazards and assumptions. All these come out of the FHA. [Ref SSA Chapter 2]
- A description of the system architecture with the Safety Requirements allocated to system elements. All these come out of the PSSA. [Ref SSA Chapter 2]
- The results of the SAEC activity.
- SSA Chapter 3 Guidance Material A.

The reviewer should verify that the Assurance and Evidence for following verification items is clearly identified in the SSA results: [Ref SSA Chapter 3 §3.1]. A requirement is deemed to be 'satisfied' when there is evidence available to show that it has been met by the new system or the change to the existing system.

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.2.1	**Assumptions are satisfied** Is evidence available to show that assumptions are satisfied?		
SSA 5.2.2.1	**Safety Requirements for people are satisfied as planned.** Is evidence available to show that Safety Requirements (including HAL) allocated to Human are satisfied?		
SSA 5.2.2.2	**Safety Requirements for procedures are satisfied, and the associated PAL is satisfied as planned.** e.g. Is evidence available to show that the Safety Requirements allocated to procedures (including PAL) are satisfied?		
SSA 5.2.2.3	**Safety Requirements for equipment are satisfied and the associated HWAL and SWAL are satisfied as planned.** e.g. Is evidence available to show that the Safety Requirements allocated to hardware and software (including HWAL and SWAL) are satisfied?		
SSA 5.2.2.4	**The interactions within the system and interaction between the system and its environment are satisfied.** e.g. Is evidence available to show that changes to airspace design have been evaluated against the adjacent areas/sectors of operations? e.g. Is evidence to show that Safety Requirements about interactions with adjacent centres are satisfied?		
SSA 5.2.3	**Safety Objectives are satisfied as planned.** e.g. Is evidence available to show that the predicted/measured frequency of occurrence of hazards resulting from system failures meet the Safety Objectives?		
SSA 5.2.4	**The risk is acceptable.** e.g. Is evidence available to show that the risks have actually been assessed and a statement of acceptance (or otherwise) by the ANSP included?		

Table 5.2A System implementation & integration

Traceability:

The reviewer should verify that the following information is clearly traceable in the SSA:

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.2.5.1	**Safety Requirements to SAEC** e.g. Can the specific assurance activities and associated evidence indicating that the Safety Requirements are met, be clearly identified?		
SSA 5.2.5.2	**Safety Objectives to SAEC** e.g. Can the specific assurance activities and associated evidence indicating that the Safety Objectives are met, be clearly identified?		
SSA 5.2.5.3	**Assumptions to SAEC** e.g. Can the specific assurance activities and associated evidence indicating that the assumptions are met, be clearly identified?		

Table 5.2B System implementation & integration

5.3 Transfer to operations verification process

The purpose of verification for this phase is to provide assurance that the system continues to meet its Safety Objectives and Safety Requirements in operation.

Verification activities started during the implementation and integration will continue. This is to obtain assurance that the system and its elements meet the associated Safety Objectives and Safety Requirements – assurance that cannot be fully obtained during implementation and integration. Note that some essential evidence can be provided during the actual transfer into operation phase (for some Safety Requirements, satisfaction can not be demonstrated in a simulated environment). [Refer SSA Chapter 3, §3.3].

The reviewer should verify that the following information is clearly identified in the SSA results: [Ref SSA Chapter 3 § 3.2]. The following table refers to verification activities of the safety assessment of the transfer into operations phase itself.

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.3.1	**Assurance & Evidence available showing that transfer phase Safety Requirements for the installation of different equipment or change of procedure are met.**		
SSA 5.3.2	**Assurance & Evidence available showing that risks induced by transfer phase on on-going ANS operations are acceptable.** e.g. Has the operating authority been appraised of the risks and indicated acceptance?		

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.3.3	**Definition of safety performance indicators.** e.g. Has the operating authority been informed which system parameters need to be monitored for safety?		
SSA 5.3.4	**Monitoring of performance of the transfer into operation phase.** e.g. Have arrangements been made to ensure that the performance of the system is verified in the operational environment?		
SSA 5.3.5	**Constraints when interfacing other systems identified and documented.** e.g. Have arrangements been made to recover to the existing system should a problem occur with the new system during transfer to operations?		

Table 5.3A Transfer to operations

The following table refers to additional (complementary) verification of Table 5.2A to be gathered during the transfer into operations phase.

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.3.6	**Limitations proposed if new safety related problems are highlighted.** e.g. The operating range of a surveillance system may have to be curtailed if positional accuracy is affected by reflections.		
SSA 5.3.7	**Monitoring of performance of the transfer into operation phase.**		
SSA 5.3.8	**Safety Objectives are satisfied as planned.** Additional to 5.2.3		
SSA 5.3.9	**Safety Requirements for people are satisfied as planned.** Additional to 5.2.2.1.		
SSA 5.3.10	**Safety Requirements for procedures are satisfied, and PAL satisfied as planned** Additional to 5.2.2.2.		
SSA 5.3.11	**Safety Requirements for equipment are satisfied, and HWAL & SWAL satisfied as planned.** Additional to 5.2.2.3.		
SSA 5.3.12	**Assumptions satisfied.** Additional to 5.2.1.		
SSA 5.3.13	**The risk is acceptable.** Additional to 5.2.4.		

Table 5.3B Transfer to Operations

5.4 Operation and maintenance verification process

The reviewer will need the correct version of the following information for conducting the verification:

- SSA - results of safety assessment of operations and maintenance.
- SSA - Chapter 3 SAEC.

The reviewer should verify that Assurance & Evidence for the following verification items is clearly identified in the SSA results: [Ref SSA Chapter 3, § 3.3.]

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.4.1	**Continuous safety monitoring is performed to ensure that Safety Requirements are met, Safety Objectives are satisfied and assumptions are correct while the system is in operation.**		
SSA 5.4.2	**Continuous safety occurrence reporting and assessment is performed.**		
SSA 5.4.3	**The risk is continuously monitored for acceptability.**		
SSA 5.4.4	**Use is made of "lessons learned", to complement formal safety occurrence reporting & assessment.**		
SSA 5.4.5	**Safety surveys are conducted.**		
SSA 5.4.6	**Safety assessment of maintenance intervention is performed.**		

Table 5.4 Operation and Maintenance

5.5 System change verification process

Any change shall be assessed decide whether it deserves or not a safety assessment or only to revisit the existing safety assessment (See Part IV Guidance Material H)

As long as the to the system and its elements (people, procedures, equipment) change deserves a safety assessment, it leads to the re-iteration of the overall safety assessment process, through the FHA, PSSA and SSA (thus no specific guidance is dedicated to this item in the SSA verification).

5.6 Decommissioning verification process

The purpose of verification for this phase is to provide assurance that the risks associated with decommissioning the system are acceptable.

The reviewer will need the correct version of the following information for conducting the verification:

- SSA - results of safety assessment of the decommissioning process;
- SSA - Chapter 3 SAEC.

The reviewer should verify that Assurance & Evidence for the following verification items is clearly identified in the SSA results: [Ref SSA Chapter 3, § 3.5.]

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.6.1	**The safety impact on global ANS operations due to withdrawing the system from operations has been assessed.**		
SSA 5.6.2	**The safety assessment of the decommissioning process itself has been performed to ensure that that risks induced on on-going ANS operations by the decommissioning operations are acceptable**.		

Table 5.6 Decommissioning

6 SSA Validation

6.1 Objective

The validation task aims at reviewing and analysing the results of the SSA to confirm that the outputs of the SSA process are correct and complete ("getting the right output"), i.e. that:

- The safety Assurance & Evidence are (and remain) correct and complete;
- All safety-related assumptions are (and remain) correct and complete.

[Ref SSA Chapter 4 - SSA Evaluation]

Note: One major aspect of Validation consists in ensuring the credibility and sensitivity of Assurance & Evidence aiming at demonstrating a certain type of satisfaction.

Note: It is assumed that Safety Objectives completeness and correctness at the system definition phase is ensured in the FHA (Chapter 4).

Note: It is assumed that Safety Requirements completeness and correctness at the system design phase is ensured in the PSSA (Chapter 4)

6.2 System implementation & integration validation process

The purpose of validation for this phase is to provide assurance that the risk of operating the new system or the change to the existing system is acceptable.

The reviewer will need the correct version of the following information for conducting SSA validation:

- A description of the high level functions of the system, with their associated Safety Objectives and a list of hazards and assumptions. All these come out of the FHA.
- A description of the system architecture with the Safety Requirements allocated to system elements. All these come out of the PSSA.
- Results of SSA verification.
- Results of Safety Assurance & Evidence Collection (SAEC).
- SSA Plan.
- SSA Generic Activities - Chapter 3 Guidance Material A.
- SSA Activities Along the Life-Cycle –Chapter 3 Guidance Material B.

The validation goals are summarised in Figure 6.2.

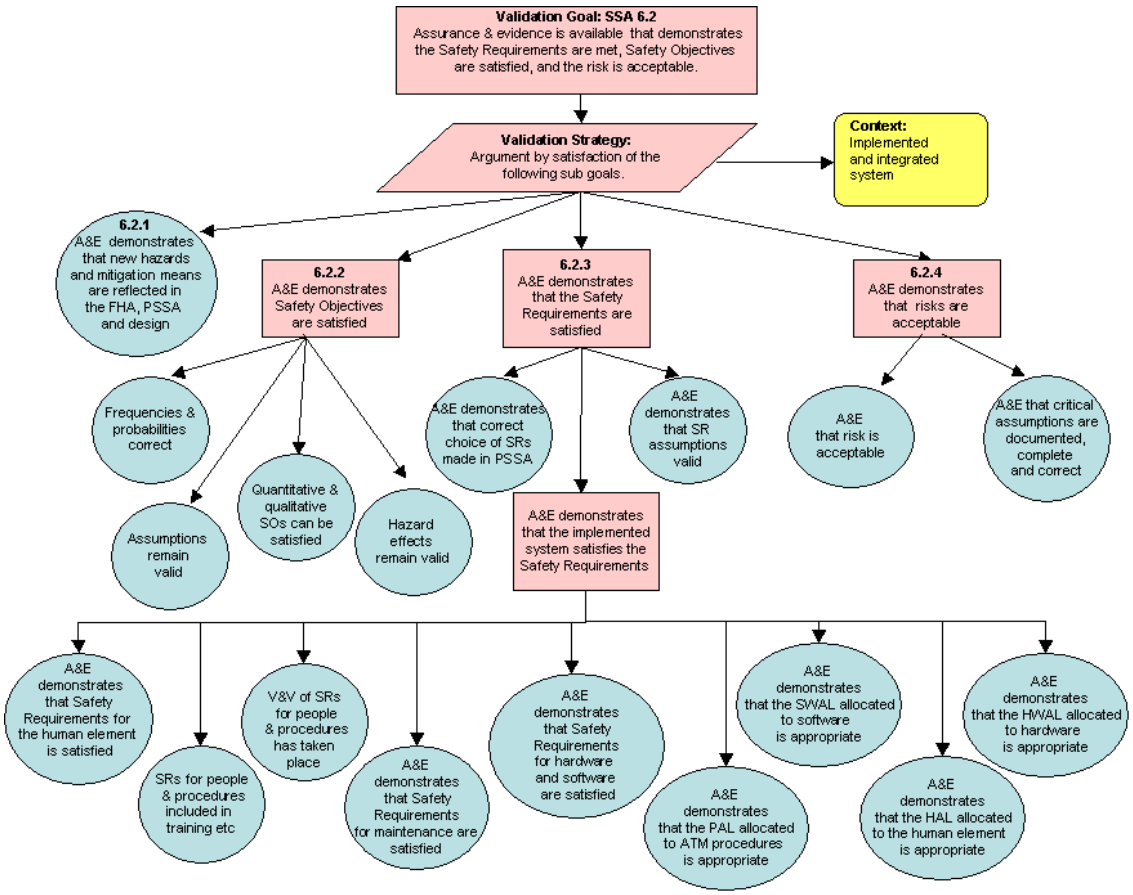

Figure 6.2: System implementation validation goals

6.2.1 New hazards and mitigation means.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.1.1	**If any new hazards and mitigation means were identified during SSA then:** **(1) the necessary revision of the FHA and/or PSSA took place or is planned; and** **(2) the necessary reiteration of the design took place or is planned.** The primary concern is that all the potential hazards arising from the system implementation and integration are identified and that appropriate mitigation is applied. One specific source of new hazards can be the unintended implemented functions (functions being implemented but not required due to e.g. reuse of or configurable elements,. [Refer to SAM Part IV GM E "Recommendations for ANS SW" Objective 3.0.4]	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.2A System implementation

6.2.2 Safety Objectives are satisfied as planned.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.2.1	**Assurance and Evidence are correct and complete to show that the quantitative frequencies and probabilities are still correct**. [Refer to SSA Chapter 3 Guidance Material B § 2.1] Reviewing analysis of the system low level design may reveal that the frequency of hazards occurring is higher than originally predicted.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.2.2	**The assumptions on which the Safety Objectives were founded remain valid, and if not that the necessary redefinition of the system took place, or is planned.** [Refer to SSA Chapter 3 Guidance Material B § 2.1]**.** Only documented assumptions are relevant – there should be no implicit assumptions.	Satisfactory ☐ Requires ☐ Action:
	Comment / action: **Reference in SSA**	
SSA 6.2.2.3	**Assurance and Evidence are correct and complete* to show that the quantitative and qualitative Safety Objectives can be satisfied as required**. [Refer to SSA Chapter 3 Guidance Material B § 2.1.1] *: At this phase of the lifecycle, it can be difficult to confirm that Safety Objectives are satisfied as they relate to a particular operational environment and limited evidence/feedback may be available/collected about that operational environment. Some confidence can be gained in this regard by establishing that the assumptions made at the outset remain valid as planned.	Satisfactory ☐ Requires ☐ Action:
	Comment / action: **Reference in SSA**	
SSA 6.2.2.2	**Assurance and Evidence are correct and complete to show that the specified probability that the hazard generates an effect (Pe) is satisfied.** Requirements set on the external mitigation means that contributed to set such Pe are satisfied. Depending on the approach chosen to set Safety Objectives either only the Pe of the Worst Credible effect has to be validated or the Pe of effect [See FHA Chapter Guidance Material G]	Satisfactory ☐ Requires ☐ Action:
	Comment / action: **Reference in SSA**	

Table 6.2B System implementation

6.2.3 Safety Requirements are satisfied as planned.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.3.1	**Assurance and Evidence are correct and complete to show that the correct choice of Safety Requirements was made during the PSSA including the correctness of the frequencies and the probabilities.** New Safety Requirements may be generated as a result of the better understanding of the system gained during the design phase.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.2	**The assumptions on which the Safety Requirements were founded remain valid, and if not that the necessary redesign of the system took place, or is planned.**	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.3	People: **Assurance and Evidence are correct and complete to show that any Safety Requirements for the human element are satisfied as required.** [Refer to SSA Chapter 3 Guidance Material B § 2.1.2] Review of credibility and sensitivity of Assurance & Evidence showing that Human Safety Requirements are satisfied such as specific training, licensing, staff selection & management, and manuals. (including HAL[1] (Human Assurance Level) satisfaction means)	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.4	ATM Procedures: **Assurance and Evidence are correct and complete to show that any the Safety Requirements for the people & procedures (including PAL) element are satisfied as required.** [Refer to SAM Part IV Annex G (SAAP) and SSA Chapter 3 Guidance Material B § 2.1.2] Review of credibility and sensitivity of Assurance & Evidence showing that ATM procedure Safety Requirements are satisfied such as procedure tasks analysis, deviation analysis, contingency plan, … Review of credibility and sensitivity of Assurance & Evidence showing that ATM procedure PAL (Procedure Assurance Level) is satisfied	Satisfactory ☐ Requires ☐ Action

[1] HAL (Human Assurance Level): At the time V2.1 of V&V Guidance Material was written, HAL definition was under development. Therefore, reference to SAM Guidance Material addressing HAL is not yet available.

Goal	Validation Item:	Validation Result
	Comment / action: **Reference in SSA**	
SSA 6.2.3.5	Maintenance Procedures: **Assurance and Evidence are correct and complete to show that any Safety Requirements relating to maintenance procedures are satisfied as required**. [Refer to SSA Chapter 3 – GM C & SSA Chapter 3 Guidance Material B § 2.1.3] Review of credibility and sensitivity of Assurance & Evidence showing that each maintenance procedure satisfies its safety requirements (for example as defined in the Maintenance Manual and Training Programme).	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.6	Equipment**: Assurance and Evidence are correct and complete to show that any Safety Requirements relating to hardware (including HWAL) and software (including SWAL) are satisfied as required**. [Refer to SAM- Part IV Annex F & SSA Chapter 3 Guidance Material B § 2.1.4] Review of credibility and sensitivity of Assurance & Evidence showing that: The hardware satisfies its HWAL (Hardware Assurance Level); The software satisfies its SWAL (Software Assurance Level).	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.7	**Assurance and Evidence are correct and complete to show that the PAL allocated to any ATM procedure is appropriate.** [Refer to SAM Part IV Annex G (SAAP) and PSSA Chapter 3 Guidance Material A] Review of the credibility and sensitivity of Assurance & Evidence sustaining the PAL allocation.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.8	**Assurance and Evidence are correct and complete to show that the SWAL allocated to any software is appropriate.** [Refer to SAM Part IV Annex F (Recommendations for ANS SW) and PSSA Chapter 3 Guidance Material A] Review of the credibility and sensitivity of Assurance & Evidence sustaining the SWAL allocation.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Goal	Validation Item:	Validation Result
SSA 6.2.3.9	**Assurance and Evidence are correct and complete to show that the HWAL allocated to any hardware is appropriate.** Review of the credibility and sensitivity of Assurance & Evidence sustaining the HWAL allocation, if any.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.10	**Assurance and Evidence are correct and complete to show that the HAL allocated to any human element is appropriate.** [Refer to TBD] [2] At the time this V&V Guidance Material was written HAL was under development. Review of the credibility and sensitivity of Assurance & Evidence sustaining the HAL allocation.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.2C System implementation

6.2.4 The risk is acceptable.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.4.1	**Assurance and Evidence are correct and complete to show that the risk is acceptable.** Review of the credibility and sensitivity of Assurance & Evidence showing that risk is acceptable. The demonstration may have to rely on system knowledge and data available at that stage of the lifecycle [Refer to SSA Chapter 3 Guidance Material A § 2.3.1] Note: Demonstration that risk is acceptable can not always be fully made during this phase (sensitivity analysis to certain remaining SRs or SOs not yet fully satisfied can be made).	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.4.2	**Any critical assumptions about the system, its operational environment and its regulatory framework are justified, documented, complete and correct.** For example, if the system design required that data lines should have dual independent routing and the lines were supplied by a third party it would be insufficient just to assume that they complied with the requirement.	Satisfactory ☐ Requires ☐ Action:
	Comment / action: **Reference in SSA**	

Table 6.2D System implementation

6.3 Transfer to operations validation process

The purpose of validation for this phase is to provide assurance that the transfer into operation risk is acceptable.

The reviewer will need the correct version of the following information for conducting the validation:

- SSA - verification results.
- SSA - Guidance Material along the life cycle.
- SSA - results of safety assessment of the transfer into operations.

The validation goals are summarised in Figure 6.3:

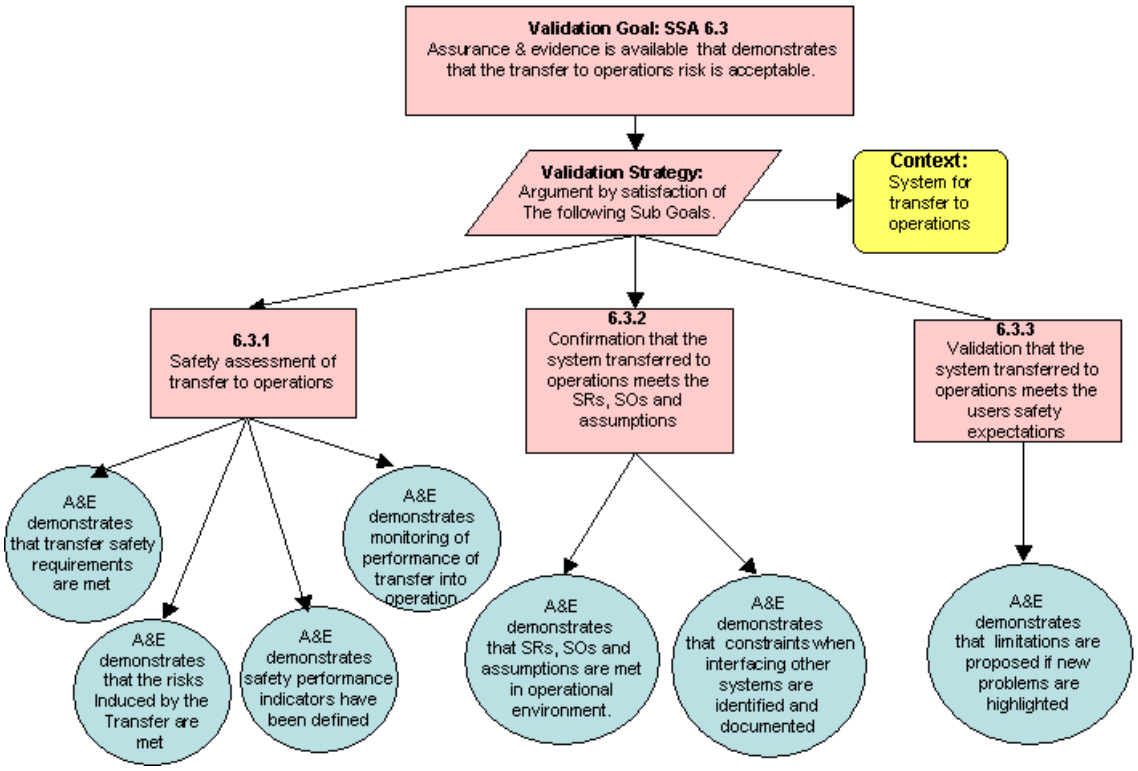

Figure 6.3 System transfer to operations validation goals

6.3.1 Safety assessment of transfer into operations.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.3.1.1	**Assurance and Evidence are correct and complete to show that the transfer phase' Safety Requirements for the installation of different equipment or change of procedure are satisfied as required.** [Refer to Guidance Material B § 2.2.2] Review of the credibility and sensitivity of Assurance & Evidence showing that these Safety Requirements are met. It needs to be planned and managed by the ANSP, and there should be evidence to that affect.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.3.1.2	**Assurance and Evidence are correct and complete to show that the risks induced by transfer phase on on-going ANS operations are acceptable.** Review of the credibility and sensitivity of Assurance & Evidence showing that transfer into operation phase risk is acceptable. The ANSP should be fully aware of what the risks are. It needs to be planned and managed, and there should be evidence to that affect.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.3.1.3	**Safety performance indicators are credible, correct and have the appropriate coverage (representative system, traffic load and duration).** Safety performance indicators should be linked to Safety Objectives; safety is only meaningful in an operational context. Safety performance indicators should be usable in ongoing risk assessment.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.3.1.4	**Monitoring of performance of the transfer into operation phase.** The ANSP should be fully aware of what the performance requirements are. It needs to be planned and managed, and there should be evidence to that affect.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.3A Transfer to Operations phase itself

6.3.2 Confirmation that the system, as transferred into operation, meets the Safety Requirements, Safety Objectives and that the assumptions are correct.

The following table refers to additional (complementary) validation of Table 6.2B, C & D to be gathered during the transfer into operations phase.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.3.2.1	**Assurance and Evidence are correct and complete to show that the Safety Requirements, Safety Objectives and all assumptions are met in the actual operational environment.** [Ref SSA Chapter 3 Guidance Material B § 2.2.2.] This is an ongoing process, requiring review of the system performance by the ANSP.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.3.2.2	**Constraints when interfacing other systems are identified and documented.** For example, if the facilities that the system depends on (Power Supply, Heating, Ventilation, etc) are managed by a third party under contract to the ANSP, then the principles and procedures by which the contractors operate the system need to be agreed and documented in order to minimise the risk of unscheduled impacts on the system.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.3B Transfer to operations

6.3.3 Validation of the system as transferred into operations with respect to users' safety expectations.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.3.3.1	**Limitations are proposed if new safety related problems are highlighted.** [Refer to SSA Chapter 3 Guidance Material B § 2.2.3.] For example, the operating range of a surveillance system may have to be curtailed if positional accuracy is affected by reflections in one sector of operations.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.3C Transfer to operations

6.4 Operation & maintenance validation process

The purpose of validation for this phase is to provide assurance that the risk continues to be acceptable in operation as indicated by system performance.

The reviewer will need the correct version of the following information for conducting the validation:

- The results of the SAEC activity;
- SSA Chapter 3 Guidance Material B - SSA activities along the life cycle.

The validation goals are summarised in Figure 6.4:

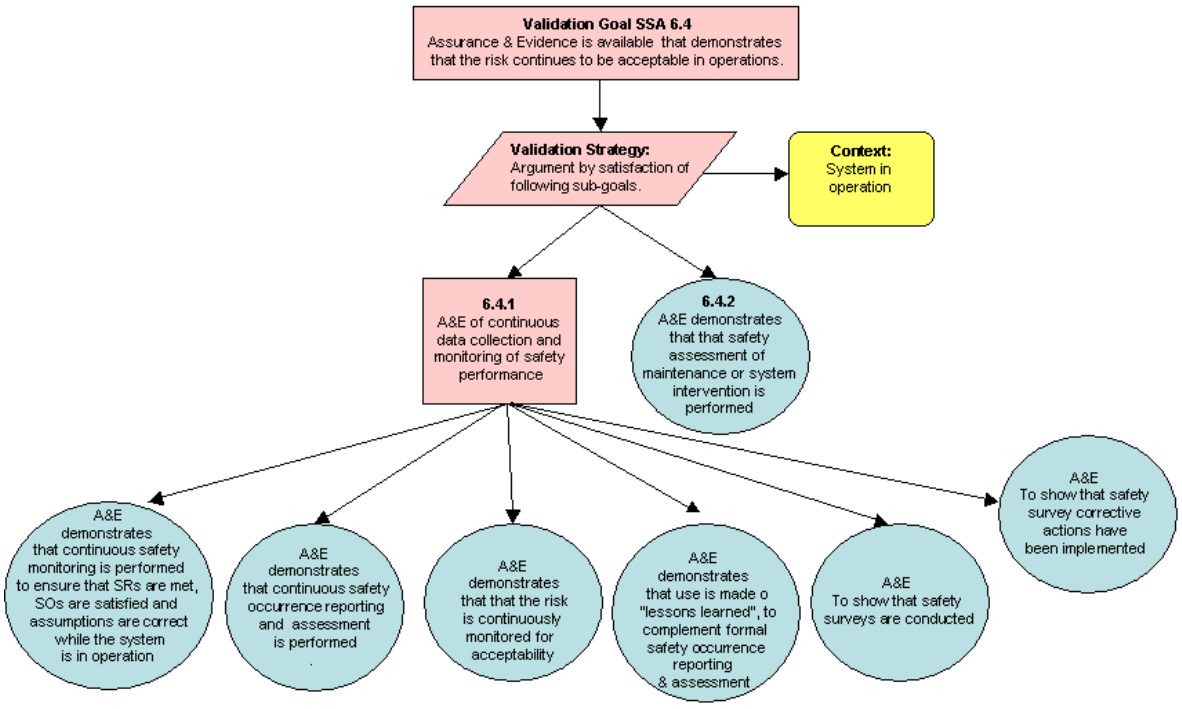

Figure 6.4 Operations and maintenance validation goals

6.4.1 Continuous data collection and monitoring of safety performance.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.4.1.1	**Assurance and Evidence are correct and complete to show that continuous safety monitoring is performed to ensure that Safety Requirements are met, Safety Objectives are satisfied and assumptions are correct while the system is in operation.** [Refer to SSA Chapter 3 Guidance Material B § 2.3] Confirmed by establishing that formal monitoring arrangements and procedures are in place, and system performance records are maintained.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.4.1.2	**Assurance and Evidence are correct and complete to show that continuous safety occurrence reporting and assessment is performed.** [Refer to SSA Chapter 3 Guidance Material B § 2.3] Confirmed by establishing that incidents are recorded, formal analysis of results takes place, and remedial action is carried out.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.4.1.3	**Assurance and Evidence are correct and complete to show that the risk is continuously monitored for acceptability**. [Refer to SSA Chapter 3 Guidance Material B § 2.3] Judged by formal arrangements and procedures in place, to assess system performance against safety objectives.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.4.1.4	**Assurance and Evidence are correct and complete to show that use is made of "lessons learned", to complement formal safety occurrence reporting & assessment.** [Refer to SSA Chapter 3 Guidance Material B § 2.3] Refers to lessons learned from ANSP's own experience but also from the wider ATM community. Evidence would include publication/availability of local information sheets or digests of occurrences.	Satisfactory ☐ Requires Action ☐

	Comment / action: **Reference in SSA**	
SSA 6.4.1.5	**Assurance and Evidence are correct and complete to show that safety surveys are conducted**. [Refer to SSA Chapter 3 Guidance Material B § 2.3] Ideally, a schedule of surveys would be agreed and planned annually taking account of available resources. The selected items for survey need not be limited to those which may be a cause for concern, as potential issues to be addressed invariably result from surveys.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.4.1.6	**Assurance and Evidence are correct and complete to show that safety survey corrective actions follow-up (including their implementation and effectiveness) is conducted**.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.4A Operation and maintenance

6.4.2 Safety assessment of maintenance and planned interventions.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.4.2	**Assurance and Evidence are correct and complete to show that safety assessment of maintenance and/or planned intervention is performed**: [Refer to SSA Chapter 3 Guidance Material C] This is a critical area, common for human error resulting in system failures. The assessment should address the ongoing adherence to procedures, the procedures themselves, and the competency of the individuals involved.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.4B Operation and maintenance

6.5 System change validation process

Any major change to the system and its elements (people, procedures, equipment) leads to the re-iteration of the overall safety assessment process, through the FHA, PSSA and SSA. Thus no specific guidance is dedicated to this item in the SSA validation.

6.6 Decommissioning validation process

The reviewer will need the correct version of the following information for conducting the validation:

- The results of the SAEC activity;
- SSA Chapter 3 Guidance Material B - SSA Activities along the life cycle.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.6.1.1	**Assurance and Evidence are correct and complete to show that the safety assessment on global ANS operations due to withdrawing the system from operations has been performed**. [Refer to SSA Chapter 3 Guidance Material B § 2.5] Have all the Safety Requirements met by the withdrawn system been addressed by the new system, or shown to be no longer valid?	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.6.1.2	**Assurance and Evidence are correct and complete to show that the safety assessment of the decommissioning process itself has been performed to ensure that the risk induced on on-going ANS operations during the decommissioning operations is acceptable.** [Refer to SSA Chapter 3 Guidance Material B § 2.5] What steps have been taken to ring fence the operational system during the decommissioning? Responsibility for protecting the operational system should not be delegated to individuals outside the ANSP and a level of supervision should be in place appropriate to the safety significance of the system.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	

Table 6.6 Decommissioning

6.7 SSA Report

The purpose of the SSA Report is to support the decision making process by providing assurance about the prospects of the system achieving an acceptable risk.

The SSA report should contain a summary of the findings, supported by marked up V&V tables and commentary.

In addition the reviewer shall confirm the following:

Goal	Validation Item:	Validation Result
SSA 6.7.1	**Assurance and Evidence are correct and complete to show that Personnel conducting the safety assurance are suitably qualified.** They should be familiar with and understand the SAM recommendations.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.7.2	**The reviewer shall comment on the quality of the process followed and whether the safety assurance activities appear to be both adequate and appropriate**. This is for the information of the Safety Manager so that improvements can be made to the process as necessary. To review Safety Evidence, the following criteria have been appropriately covered (an acceptable rationale exists to sustain the choices made to address those criteria): • All Safety Requirements are continuously satisfied with the appropriate level of demonstration; • All Safety Objectives are continuously satisfied; • Risk is continuously acceptable; • Documentation and Evidence are up-to-date with regards actual operations.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.7 SSA Report